Active Directory in the COE

2 November 2001

Eric L. Krum
NTAG Co-chair
781.271.5144
krume@mitre.org

Purpose

- To provide information on Active Directory in the COE

Outline

- Active Directory Overview
- Draft I&RTS Directory Services Chapter
- Conclusion
- Future Directions of Active Directory

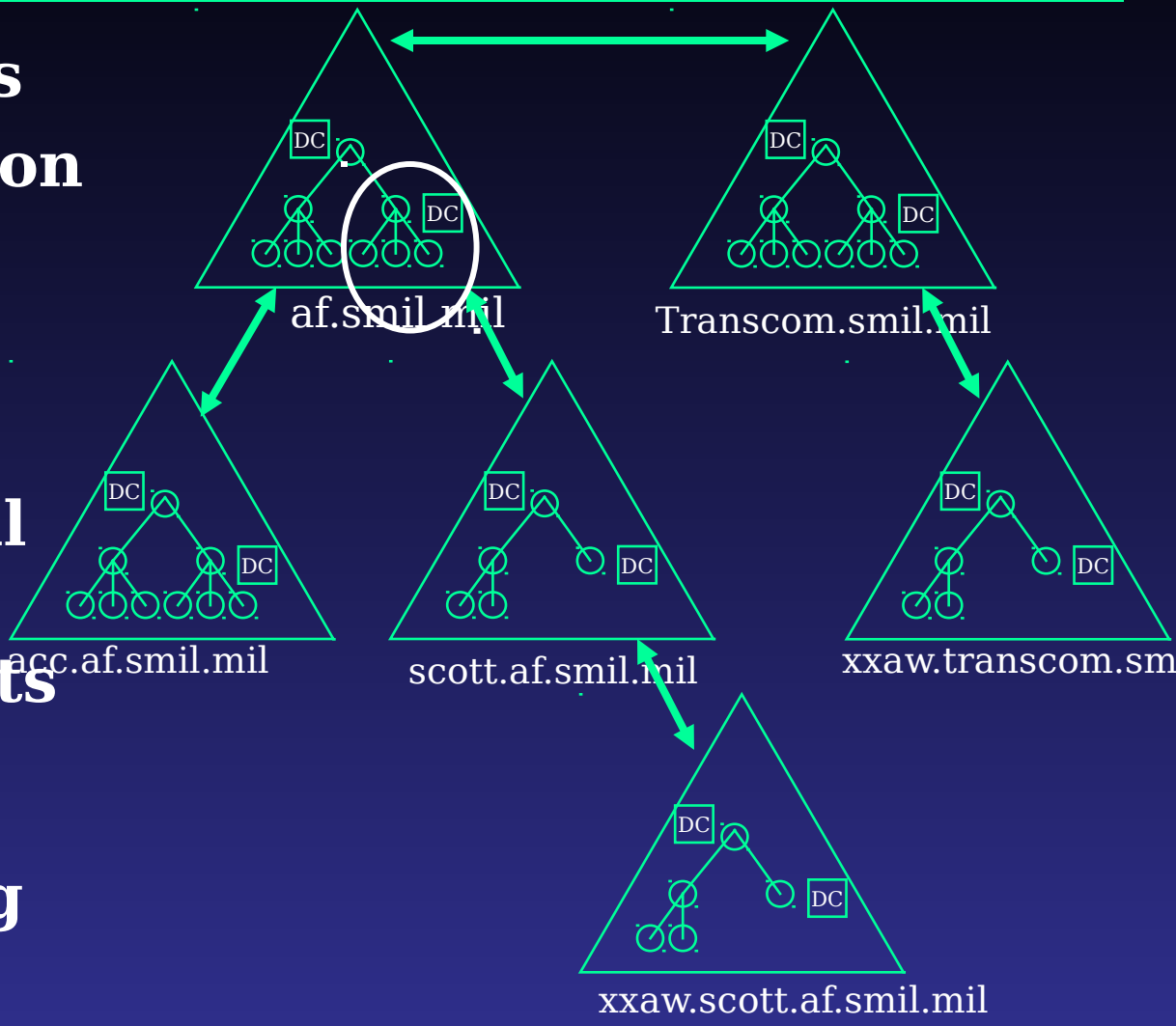
What is Active Directory?

Active Directory is an integral part of Windows 2000 Server that delivers essential network operating system services:

- LDAP v3 directory implementation
- Focal point for management of network elements (users, applications, devices, etc.)
- Trusted repository of security data for authentication and authorization
- Platform for application development and integration with other systems

Active Directory Concepts

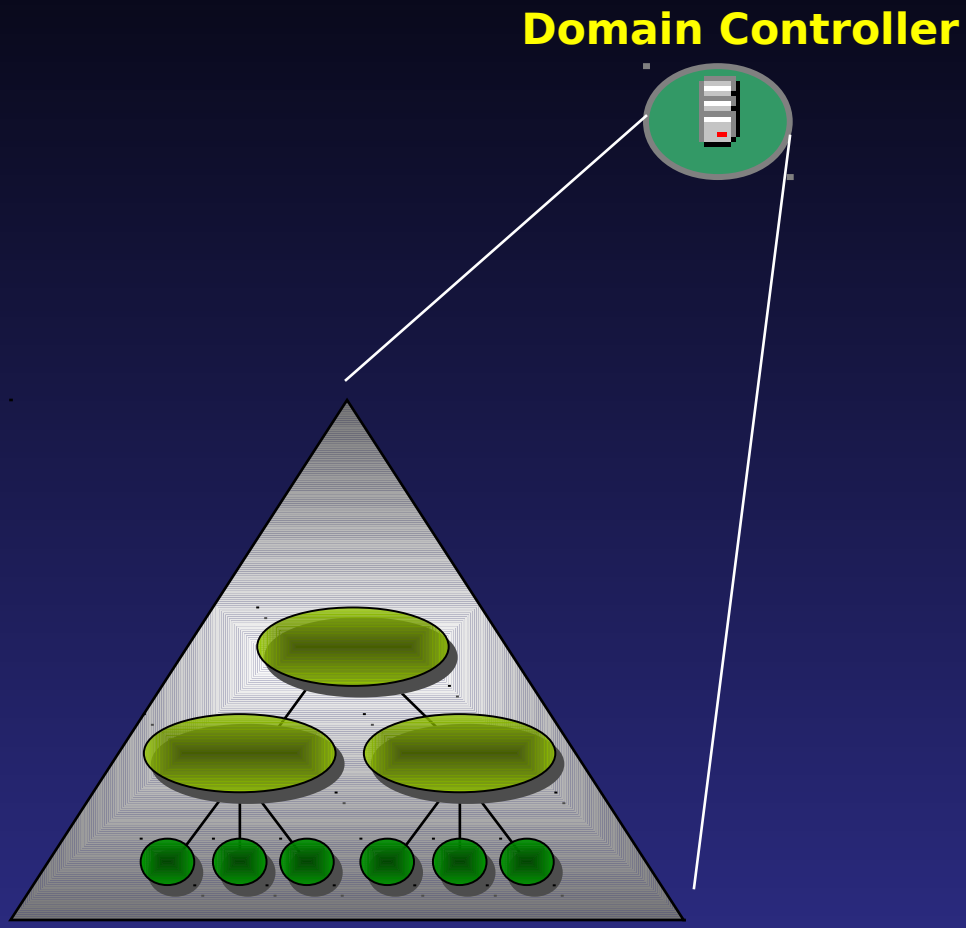
- **Logical Concepts**
  - **DNS Integration**
  - **Domains**
  - **Tree**
  - **Forest**
  - **Organizational Units**
- **Physical Concepts**
  - **Domain controllers**
  - **Global Catalog**
  - **Replication**
  - **Sites**



Note: A WinNT 4.0 Domain == Windows 2000 Domain == D

Domains
Basis of AD Structure

- Security boundary
- Scopes:
  - Policy
  - Access Control
- Top level container in an X.500-like tree
  - Partition of the enterprise-wide directory service
- Default Kerberos V5 authentication
- DNS is used to locate domain controllers



Domain Controllers

- Master roles
  - Schema master (forest)
  - Domain naming master (forest)
  - Relative Identifier (RID) master (domain)
  - Infrastructure master (domain):
  - Primary domain controller (PDC) emulator (domain)
- Domain Controllers with a Global Catalog
  - holds all objects from all domains in the forest/tree, as well as a subset of each object's properties.

Global Catalog

Domain Schema

- User Account
  - Name
  - Title
  - Manager
  - Office Location
  - Phone
  - Division
  - Cost Center Code
  - Certification Expires
- Printer
  - Name
  - Mfr
  - Model
  - Color
  - Duplex

Global Catalog

- User Account
  - Name
  - Title
  - Manager
  - Office Location
  - Phone
- Printer
  - Name
  - Mfr
  - Model

Allows Rapid Searches

Read Only

Active Directory Schema

- Active Directory schema contains two primary items:
  - object class
  - attribute
- Object class represents a category of objects that share a set of common characteristics
- Attributes used to describe instances of the class

Active Directory Schema (2)

- Attributes are classified as mandatory and optional
- Linked Attributes - can link a new attribute to an existing attribute, e.g.,
  - User Manager => User Reports
  - Links must have a unique link identifier.

Schema Structure (3)

- Object Identifier (OID)
  - Must be unique for all directories
  - Issued by ISO who owns the international LDAP root OID
  - ANSI issues OIDs in North America for ISO
    - **1.2.840**
  - Microsoft has a root OID from ANSI
    - **1.2.840.113556**
  - Microsoft does issue OID roots to companies that are derived from their root
  - Number of root OIDs is a performance issue. Goal should be to minimize the number of root OIDs.

Extending the Schema

- Derive a new subclass from an existing class
  - Use existing attributes
  - Add new attributes to new subclass
- Add additional attributes to an existing class
- Create an entirely new class with new attributes

Security Model

- Negotiate an authentication mechanism
- Access Control Lists (ACLs)
  - Objects
  - Attributes
- Can grant or deny access, i.e., Create Child, Delete Child, Read Property, Write Property
- Signing and Sealing LDAP
  - Encryption via the Kerberos Session Key

Port Numbers

- LDAP
  - 389
- LDAP SSL
  - 636
- Global Catalog – (GC)
  - 3268
- GC SSL
  - 3269

Draft I&RTS Directory Services Chapter

- Active Directory (AD) is a subsection of the Directory Services chapter
- Matches AD Guidance signed by Mr. Money on 6 April 2001
- Active Directory
  - Each Service, CINC, or agency should determine their own AD topology
  - All CINCs, Services and agency's AD implementations shall share a common AD global catalog schema.
  - CINCs, Services and agencies determine Universal group naming conventions
  - CINCs, Services and agencies determine distribution group naming conventions

Draft I&RTS Directory Services Chapter(2)

- The Logo Program *Application Specification for Microsoft Windows 2000 Servers* directs naming conventions for extending the AD schema.
  - Common-Name (cn),
    [DNS]-[prefix]-[Application or System name]-[Description]
  - LDAP-Display-Names (lDAPDisplayName)
    - [DNS]-[prefix Application or System name Description]
  - Globally Unique Identifier (GUID), and
    - Created by developer
  - Object Identifiers (OIDs).
    - The appropriate service, agency, or CINC determines the source for their OID root and policies for controlling OIDs derived from the root.

Draft I&RTS Directory Services Chapter(3)

- Cognizant Chief Engineer shall approve all schema changes
- AD schema changes shall be coordinated with the DISA Chief Engineer for Directory Services prior to implementation.
- Schema change applications are not required to have a Logo Certificate from Microsoft

Draft I&RTS Directory Services Chapter(4)

- AD aware application developers may obtain OIDs and link-Id's from the DISA Engineering Office.
- Include the DoD Electronic Data Interchange_Personal Indicator (EDI_PI) issued by the Manpower Data Center
  - Support of CAC
  - EDI_PI used as UserPrincipleName (UPN) prefix
  - Log in maybe EDI_PI@mil

Active Directory Considerations

- Except for security issues, same requirements for all directories. Implementation details differ.
- Establishment of operations to implement AD requirements in draft Chapter 10.
- Use of directory enabled segments
  - Standard submittal package
  - Schema implementation segment

Active Directory Considerations (2)

- Use of Microsoft Certificate Server for machine certificates enrolled in Win2k domains. Enhances security and administration.
- Use of directories to locate services on network
- Controlling Quality of Service (QoS)
- Use of Dynamic DHCP with AD

Active Directory Considerations (3)

- APM Windows domain account integration
  - AD domain controller PDC emulator role responds to all NT domain calls
  - Can use LDAP v3 API or AD Service Interfaces (ADSI) to access AD
- COE standard domain Group Policy Object
- iPlanet directory and AD common schema requirements
- Only one forest can be the authority for a UPN suffix. @mil for all account will cause conflicts in forest trusts.

Active Directory Considerations (4)

- NSA security guides
  - Guide to Securing Microsoft Windows 2000 Schema
  - Guide to Securing Microsoft Windows 2000 AD (Win2k_DC.inf)
  - Guides available at: http://nsa1.www.conxion.com
- Kerberos v5 (IETF RFC 1510)
  - Supports account authentication
  - Limited for account or group authorization

Conclusion

- AD is a Complex Topic
- Draft I&RTS Provides AD Guidance
- Next Steps:
  - Solicit Community Involvement on Solutions
  - Future Direction of AD and Windows OSs

Future Directions of Active Directory

- Windows .NET Servers due for release first half 2002
- Ability to delete schema
- Remove need to do a full synch when adding a Global Catalog attribute
- Domain renaming
- Forest restructuring
- Cross-Forest Trust

Future Directions of Active Directory (2)

- Resultant Set of Policy (RSoP)
  - Two modes:
    - Logging Mode: What policies applied?
    - Planning Mode: What policies will apply?
- Restore Default Group Policy Object Tool
- Replicate groups by member instead of by group
- Eliminates the limit of 5000 direct group members

Future Directions of Active Directory (3)

- Users are able to logon without contacting Global Catalog Server
- Create domain controller from media
- Support for *inetOrgPerson* class
  - Can be used as a security principal
- Microsoft Metadirectory Services being incorporated into AD